Security Products

ISG 2000
Hardware Installation and Configuration Guide

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Part Number: 093-1937-000, Revision C

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Table of Contents

About This Guide

The Juniper Networks ISG 2000 is a purpose-built, high-performance security device designed to provide a flexible solution to medium and large enterprise central sites and service providers. The ISG 2000 security device integrates firewall, deep inspection (DI), virtual private network (VPN), and traffic management functionality in a low-profile, modular device.

Built around a fourth-generation security ASIC, the GigaScreen3, which provides accelerated encryption algorithms, the ISG 2000 supports flexible interface configuration with the following interface options for its four open slots:

- 10/100 Mbps interface module, for 10/100Base-T connections (four and eight ports)
- 10/100/1000 Mbps interface module, for 10/100/100Base-T connections (two ports)
- Mini-GBIC interface module, for fiber-optic connections (two and four ports)

NOTE: The configuration instructions and examples in this document are based on the functionality of a device running ScreenOS 6.1.0. Your device might function differently depending on the ScreenOS version you are running. For the latest device documentation, refer to the Juniper Networks Technical Publications website at www.juniper.net/techpubs/hardware. To see which ScreenOS versions are currently available for your device, refer to the Juniper Networks Support website at http://www.juniper.net/customers/support/.

Organization

This guide includes the following sections:

- Chapter 1, “Hardware Overview,” describes the device and components of an ISG 2000 device.
- Chapter 2, “Installing and Connecting a Device,” describes how to mount and connect cables and power to an ISG 2000 device.
- Chapter 3, “Configuring a Device,” describes how to configure and manage an ISG 2000 device and how to perform some basic configuration tasks.
- Chapter 4, “Intrusion Detection and Prevention,” describes how to connect the Intrusion Detection and Prevention (IDP) security modules into an ISG 2000 device.
- Chapter 5, “Servicing a Device,” describes service and maintenance procedures for an ISG 2000 device.
- Appendix A, “Specifications,” provides general device specifications for an ISG 2000 device.

Conventions

This guide uses the document conventions as described in the following sections:

- “Web User Interface Conventions” on page 6
- “Command Line Interface Conventions” on page 7

Web User Interface Conventions

The Web user interface (WebUI) contains a navigational path and configuration settings. To enter configuration settings, begin by clicking a menu item in the navigation tree on the left side of the screen. As you proceed, your navigation path appears at the top of the screen, with each page separated by angle brackets.

The following example shows the WebUI path and parameters for defining an address:

Policy > Policy Elements > Addresses > List > New: Enter the following, then click **OK**:

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask: (select), 10.2.2.5/32
Zone: Untrust

To open online Help for configuration settings, click the question mark (?) in the upper left of the screen.

The navigation tree also provides a Help > Config Guide configuration page to help you configure security policies and Internet Protocol Security (IPSec). Select an option from the list and follow the instructions on the page. Click the **?** character in the upper left for Online Help on the Config Guide.

Command Line Interface Conventions

The following conventions are used to present the syntax of command line interface (CLI) commands in text and examples.

In text, commands are in **boldface** type and variables are in *italic* type.

In examples:

- Variables are in *italic* type.
- Anything inside square brackets [ ] is optional.
- Anything inside braces **{ }** is required.
- If there is more than one choice, each choice is separated by a pipe (|). For example, the following command means "set the management options for the ethernet1, the ethernet2, *or* the ethernet3 interface":

```
set interface { ethernet1 | ethernet2 | ethernet3 } manage
```

NOTE: When entering a keyword, you only have to type enough letters to identify the word uniquely. For example, typing **set adm u ang j12fmt54** is enough to enter the command **set admin user angel j12fmt54**. Although you can use this shortcut when entering commands, all the commands documented here are presented in their entirety.

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/customers/support/downloads/710059.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings—http://www.juniper.net/customers/support/
- Find product documentation—http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base—http://kb.juniper.net/
- Download the latest versions of software and review your release notes—http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications—http://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum—http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Manager—http://www.juniper.net/customers/cm/
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool—https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Manager tool in the CSC at http://www.juniper.net/customers/cm/.
- Call 1-888-314-JTAC (1-888-314-5822—toll free in USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at http://www.juniper.net/customers/support/requesting-support/.

Feedback

If you find any errors or omissions in this document, contact Juniper Networks at techpubs-comments@juniper.net.

Chapter 1

Hardware Overview

This chapter provides detailed descriptions of the ISG 2000 device. It includes the following sections:

Ports and Interface Module Slots

This section describes the location of the interface module slots and built-in ports. Refer to Figure 1 for built-in port and slot locations and to Table 1 for descriptions of the ports, interface modules, and cable connectors.

Figure 1: Port and Interface Module Locations

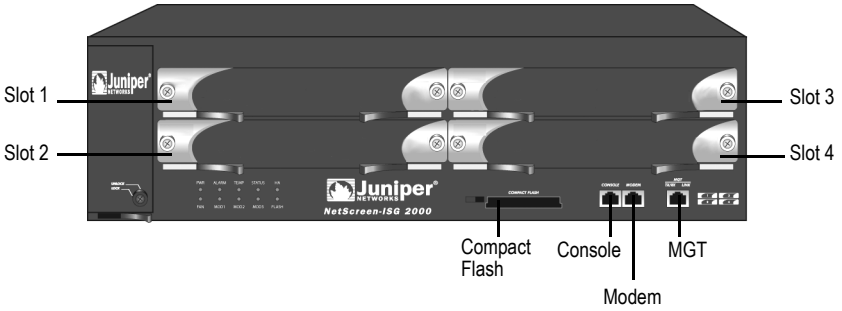


Table 1: ISG 2000 Port, Interface Modules, and Cable Connectors

Port	Description	Connector	Speed/Protocol
Console	Enables a serial connection with the device. Used for terminal-emulation connectivity to launch CLI sessions.	RJ-45	9600 bps/RS-232C serial
Modem	Enables a backup RS-232 async serial Internet connection through an external modem.	RJ-45	9600 bps — 115 Kbps/RS-232C serial
MGT	Provides a dedicated connection for management traffic.	RJ-45	10/100Base-T
Compact Flash	Allows you to download or upload device software or configuration files and to save log files.	NA	NA
Interface Modules			
FE4	4-port Fast Ethernet	RJ-45	10/100Base-T
FE8	8-port Fast Ethernet	RJ-45	10/100Base-T
GB2-TX	2-port Gigabit	RJ-45	10/100/1000Base-T
GB2-LX	2-port Mini GBIC with LX transceivers	LC	1000Base-LX
GB2-SX	2-port Mini GBIC with SX transceivers	LC	1000Base-SX
GB4-TX	4-port Mini GBIC with TX transceivers	RJ-45	10/100/1000Base-T
GB4-LX	4-port Mini GBIC with LX transceivers	LC	1000Base-LX
GB4-SX	4-port Mini GBIC with SX transceivers	LC	1000Base-SX
10GB1-SR/LR	1-port 10 Gigabit with XFP transceivers	LC	10Gbase-SR, 10Gbase-LR

Front Panel

The front panel of the ISG 2000 has the following:

- Device Status LEDs
- Port Descriptions
- Interface Modules
- Fan Tray

Device Status LEDs

The ISG 2000 device status LEDs display information about critical device functions. When the device powers up, the POWER LED changes from off to blinking green, and the STATUS LED changes in the following sequence: red, green, blinking green. Startup takes approximately two minutes. If you want to turn the device off and on again, we recommend you wait a few seconds between shutting it down and powering it back up. Table 2 provides the name, color, status, and description of each device status LED.

Table 2: Device LED Descriptions

Name	Color	Status	Description
POWER	Green	On steadily	Device is receiving power.
		Off	Device is not receiving power.
	Red	On steadily	Power supply is functioning incorrectly.
ALARM	Red	Blinking	Self-test failure occurred while ScreenOS was starting up. Certain algorithm and ACL failures can cause this. Device alarm blinks once for each software attack.
	Amber	On steadily	One of the following failures has occurred: ■ Power supply is off ■ Hardware failure ■ Error with software module
		Off	No alarm condition(s) present.
TEMP	Green	On steadily	Temperature is within 32°F (0°C) to 131°F (55°C).
	Orange	On steadily	Temperature is within 132°F (56°C) to 150°F (66°C).
	Red	On steadily	Temperature exceeds 150°F (66°C).
STATUS	Green	On steadily	Device is active.
		Blinking	Device is starting.
		Off	Device is off.
HA	Green	On steadily	Device is the primary.
	Amber	On steadily	Device is the backup.
	Red	On steadily	HA is defined; device is not the backup.
		Off	No HA activity is defined.

Name	Color	Status	Description
FAN	Green	On steadily	All fans are functioning properly.
	Red	On steadily	One or more fans failed or a fan subdevice is not receiving power.
MOD1	Green	On steadily	Interface module is installed.
		Off	No interface module is installed.
MOD2	Green	On steadily	Interface module is installed.
		Off	No interface module is installed.
MOD3	Green	On steadily	Interface module is installed.
		Off	No interface module is installed.
MOD4	Green	On steadily	Interface module is installed.
		Off	No interface module is installed.
FLASH	Green	On steadily	PC card is installed in the compact flash slot.
		Blinking	Read-write activity is detected.
		Off	Compact flash slot is empty.

Port Descriptions

This section explains the purpose and function of the following components:

- Compact Flash Slot
- Management Interfaces

Compact Flash Slot

The compact flash slot enables you to download or upload device software or configuration files and save log files to a compact flash card.

To save files to or from the device, use the following CLI command:

save { software | config } from { flash | slot1 *filename* } to { flash | slot1 *filename* }

where **flash** is the internal flash memory, **slot1** is to the compact flash slot, and *filename* is the name of the software or configuration file on the compact flash card.

Management Interfaces

The ISG 2000 offers three management interfaces:

- Console Port — This RJ-45 serial port wired as data circuit-terminating equipment (DCE) that can be used for local administration. Use a straight-through cable when using a terminal connection and a crossover cable when connecting to another DCE device. An RJ-45 to DB-9 adapter is supplied. See “Connectors” on page 65 for the RJ-45 connector pinouts.
- Modem Port — This RJ-45 serial port, wired as data terminal equipment (DTE) that can be connected to a modem to allow remote administration. We do not recommend using this port for regular remote administration. Use a straight-through cable when connecting to a modem and a crossover cable when connecting to another DTE device.
  See “Connectors” on page 65 for the RJ-45 connector pinouts.
- 10/100 MGT Port — The management (MGT) port is a fixed 10/100Base-T interface that provides a dedicated connection for management traffic. It has a separate IP address and netmask (default is 192.168.1.1/24) and can be configured with the Web user interface (WebUI) and the command line interface (CLI). The MGT port is only to be used for management purposes and is not capable of routing traffic to other interfaces.

Interface Modules

The front panel of the ISG 2000 device has four interface module slots, which can accommodate the following types of interface modules:

- 10/100 Mbps
- 10/100/1000 Mbps
- Mini-GBIC

The modules are not hot-swappable. Your network administrator needs to determine the kinds of interfaces needed to deploy an ISG 2000 device.

When configuring one of the ports on the interface modules, refer to the interface name that corresponds to the location of the port. From left to right on the front panel, the interface names for the ports are **ethernetx/1** to **ethernetx/8**, where x is the slot number. Table 3 describes the interface module port LEDs.

Table 3: Ethernet Port LEDs

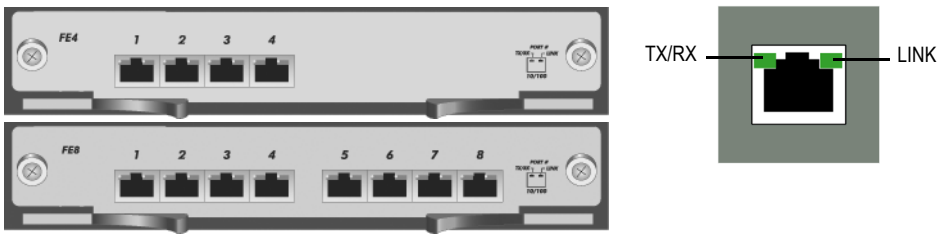
Name	Color	Status	Description
LINK	Green	On steadily	Port is online.
		Off	Port is offline.
TX/RX	Green	Blinking	Traffic is passing through. The baud rate is proportional to the link activity.
		Off	Port might be on but is not receiving data.

NOTE: To change the ALARM LED from red to green while saving the alarm message(s) in the device, use the **clear led alarm** CLI command.

10/100 Mbps Interface Module

The four-port (FE4) or eight-port (FE8) 10/100 Mbps interface module is appropriate for a 10/100Base-T LAN. Connect the ports using a crossover cable with RJ-45 connectors. Figure 2 displays the FE4 and FE8 interface module overlays and the location of the Ethernet port LEDs.

Figure 2: 10/100 Mbps Modules

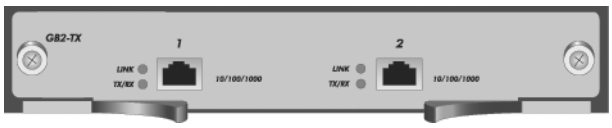


The10/100 Ethernet ports provide LAN connections to hubs, switches, local servers, and workstations. You can also designate an Ethernet port for management traffic.

10/100/1000 Mbps Interface Module

The two-port (GB2-TX) 10/100/1000 Mbps interface module is appropriate for a 10/100/1000Base-T LAN. Connect the ports using a twisted pair cable with RJ-45 connectors.

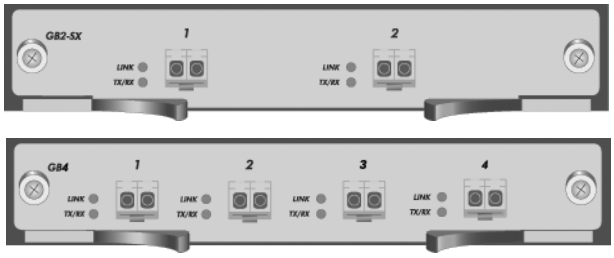
Figure 3: Fixed Two-Port 10/100/1000 Mbps Module



Mini-GBIC Interface Module

The two-port (GB2-SX or GB2-LX) and four-port (GB4) mini-GBIC interface modules provide connectivity to fiber-based and copper-based gigabit Ethernet LANs. Connect the ports using appropriate cable type depending on the specific media used. Use single-mode or multimode optical cable for SX and LX and CAT-5 cable for the 10/100/1000BaseT. See Table 13, “Interface Media Types for Mini-Gigabit Transceivers and 10Gigabit XFP Transceivers” on page 67 for a list of each media type.

Figure 4: Two-Port and Four-Port Mini-GBIC Modules



Fan Tray

The ISG 2000 device has a single hot-swappable three-fan tray, which you can access on the left front side of the chassis.

WARNING: If a fan stops operating as a result of failure or removal, the device continues to run. Do not leave the fan tray empty for more than two minutes; otherwise, heat failure or permanent damage could occur.

Back Panel

The ISG 2000 supports two redundant, fault-tolerant, auto-switching power supply units (PSUs). The PSUs are hot-swappable, so you can remove or replace one without interrupting device operation.

You can order the ISG 2000 with one or two PSUs: DC or AC. Although the ISG 2000 can run with one PSU, it is advisable to install two. This practice minimizes the chance of device failure.

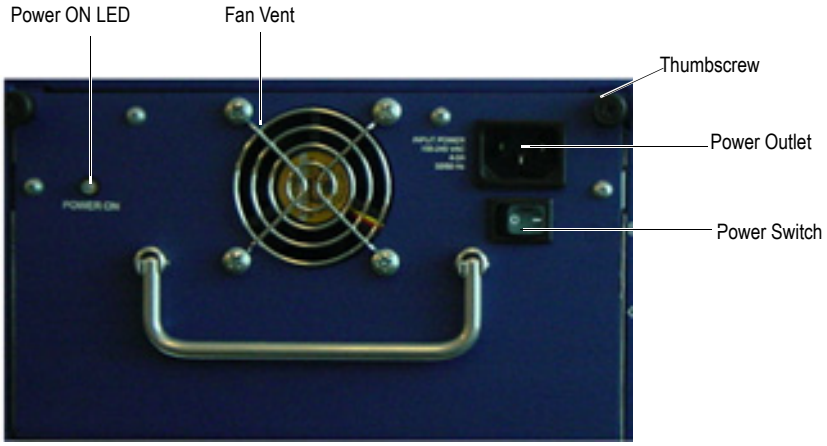
CAUTION: Do not mix the PSU types because doing so could seriously damage the device.

When the ISG 2000 contains two PSUs, they share the power load equally. If one fails, the other assumes the full load automatically and the device sends a device alarm. The POWER ON LED on the PSU only displays two colors: green, indicating that the power supply is functioning correctly, and red, which indicates that the PSU has failed.

AC Power Supply Unit

The AC PSU weighs approximately three pounds. The faceplate contains a POWER ON LED, a power switch, two thumbscrews, a cooling fan vent, and a male power outlet. Figure 5 shows the ISG 2000 AC power supply.

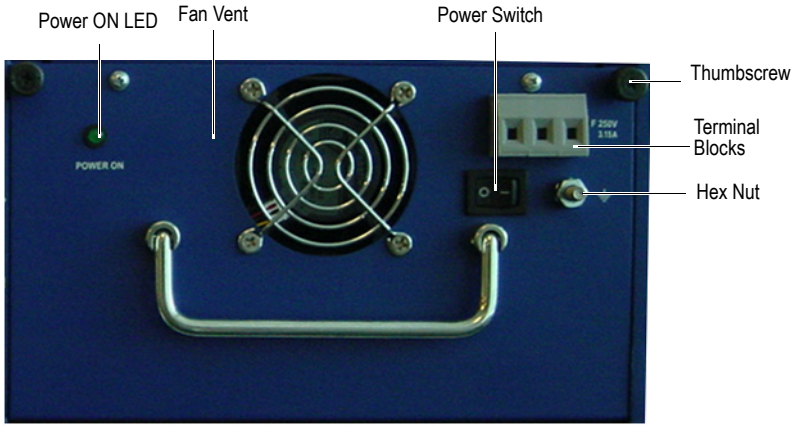
Figure 5: AC Power Supply Components



DC Power Supply Unit

The DC PSU weighs approximately three pounds. The faceplate contains a POWER ON LED, a power switch, two thumbscrews, a hex nut, a cooling fan vent, and three DC power terminal blocks that connect to power cables. Figure 6 shows the ISG 2000 DC power supply.

Figure 6: DC Power Supply Components



Chapter 2

Installing and Connecting a Device

This chapter describes how to install and connect an ISG 2000 device. It includes the following sections:

NOTE: For safety warnings and instructions, refer to the *Juniper Networks Safety Guide*. The guide warns you about situations that could cause bodily injury. When working on any equipment, be aware of the hazards involved with electrical circuitry, and follow standard practices for preventing accidents.

Before You Begin

The location of the device, the layout of the equipment rack, and the security of your wiring room are crucial for proper device operation.

WARNING: To prevent abuse and intrusion by unauthorized personnel, install the ISG 2000 device in a secure environment.

Observing the following precautions can prevent shutdowns, equipment failures, and injuries:

- Before installation, always check that the power supply unit (PSU) is disconnected from any power source.
- Ensure that the room in which you operate the device has adequate air circulation and that the room temperature does not exceed 122° F (50° C).
- Allow three feet (one meter) of clear space to the front and back of the device.
- This device is heavy. Take precautions when lifting and stabilizing the device in the rack.
- Do not place the device in an equipment rack frame that blocks an intake or exhaust port. Ensure that enclosed racks have fans and louvered sides.
- Correct these hazardous conditions before any installation: moist or wet floors, leaks, ungrounded or frayed power cables, or missing safety grounds.

Equipment Installation

The ISG 2000 comes with accessories for mounting the device in a standard 19-inch equipment rack.

Use the following guidelines while configuring your equipment rack:

- Enclosed racks must have adequate ventilation. Such ventilation requires louvered sides and a fan to provide cooling air.
- In an enclosed rack with a ventilation fan in the top, equipment higher in the rack can draw heat from the lower devices. Always provide adequate ventilation for equipment at the bottom of the rack.
- Baffles can isolate exhaust air from intake air. The best placement of the baffles depends on the airflow patterns in the rack.

Rack-mounting requires the following accessories and tools:

- Number-2 phillips screwdriver (not provided)
- Four screws to match the rack (required if the thread size of the screws provided in the ISG 2000 product package do not fit the thread size of the rack)
- Included rear slide-mount kit (for the rear-and-front-mount method)

You can install an ISG 2000 device in a center-mount or a front-rear mount configuration.

NOTE: We strongly recommend the front-rear mount configuration.

Front-Rear Mount

To front-rear mount the ISG 2000, use the rear slide-mount kit, and perform the following steps:

1. Use the screws to attach the left and right plates to the front of each side of the ISG 2000 device.
2. Use the screws to attach the rear-mount bracket to the rear-rack posts.
3. With the indented groove that runs the length of each slide facing outward, use the screws to attach the slides to the middle of each side of the ISG 2000 device.

NOTE: Depending on the depth of your equipment rack, you can attach the slides along the length of the sides or extend them over the rear of the device.

---

4. Slip the slides into the rear-mount brackets.
5. Push the ISG 2000 forward until the left and right plates contact the front rack posts.
6. Use the screws to attach the left and right plates to the rack.

Figure 7: Front-Rear Mount for ISG 2000

Center-Mount

To center-mount the ISG 2000:

1. Use the screws to attach the left and right plates to the middle of each side of the ISG 2000 device.
2. Slide the ISG 2000 in the rack.
3. Use the screws to attach the left and right plates to the rack.

Figure 8: Center-Mount for ISG 2000

Connecting the Power

This section provides installation and connection procedures for the power supply units (PSUs) available for the ISG 2000.

AC Power Supply Unit

To install and connect an AC PSU to the ISG 2000:

1. Slide the PSU into one of the power compartments in the back of the device.
2. Fasten the PSU to the device by tightening the corner screws into the eyelets on the sides of the PSU.
3. If you want to install a second PSU, repeat steps 1 and 2.
4. Connect the female end of a standard power cord to the male connector on the back of each PSU.
5. Connect each power cord to a standard 100-240-volt power outlet.

NOTE: Whenever you deploy two PSUs to an ISG 2000 device, connect each to a different power source. Each PSU is intended to receive power from separate feeds.

6. Press the power switch to the ON position.

NOTE: If there are multiple power supplies in the ISG 2000 and one of them is off, the ALARM LED on the front panel glows red. This warning indicates that maximum device reliability requires all installed power supplies to be operational.

DC Power Supply Unit

To install and connect a DC PSU to the ISG 2000:

WARNING: You must shut off current to the DC feed wires before connecting the wires to the PSUs. Also, make sure that the ON/OFF switch is in the OFF position.

1. Slide the PSU into one of the power compartments in the back of the device.
2. Fasten the PSU to the device by tightening the corner screws into the eyelets on the PSU sides.
3. Remove the hex nut on the grounding screw.
4. Place the ground lug on the screw, then tighten the hex nut securely.
5. Connect the other end of the grounding lug wire to a grounding point at your site.
6. Loosen the retaining screws on each terminal block.
7. Insert the 0V DC (positive voltage) return wire into the center COM connector and the -48V DC power-feed wire into either the left or right connector.
8. Fasten the screws over the connectors.
9. If you want to install a second PSU, repeat steps 1 through 8.
10. Press the power switch to the ON position.

NOTE: If there are multiple PSUs in the ISG 2000 device and one of them is off, the ALARM LED on the front panel glows red. This warning indicates that maximum device reliability requires all installed PSUs to be operational.

Connecting Interface Cables to a Device

To connect the interface cable to a device:

1. Have ready a length of the type of cable used by the interface.
2. Insert the cable connector into the cable-connector port on the interface faceplate.
3. Arrange the cable as follows to prevent it from dislodging or developing stress points:
    a. Secure the cable so that it is not supporting its own weight as it hangs to the floor.
    b. Place any excess cable out of the way in a neatly coiled loop.
    c. Use fasteners to maintain the shape of the cable loops.

WARNING: Certain ports on the device are designed for use as intrabuilding (within-the-building) interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Isssue 4) and require isolation from the exposed outside plant (OSP) cabling. To comply with NEBS requirements and protect against lightning surges and commercial power disturbances, the intrabuilding ports must not be metallically connected to interfaces that connect to the OSP or its wiring. The intrabuilding ports on the device are suitable for connection to intrabuilding or unexposed wiring or cabling only. The addition of primary protectors is not sufficient protection for connecting these interfaces metallically to OSP wiring.

CAUTION: To comply with intrabuilding lightning and surge requirements, intrabuilding wiring must be shielded, and the shield for the wiring must be grounded at both ends.

Connecting a Device to a Network

The ISG 2000 has four interface module slots, which can contain the following types of modules:

- 10/100 Mbps interface module, for 10/100Base-T connections (four and eight ports)
- 10/100/1000 Mbps interface module, for 10/100/100Base-T connections (two ports)
- Mini-GBIC interface module, for fiber-optic connections (two and four ports)

The type of network used by your organization determines the kind of interface needed to connect the ISG 2000. (For more information about interface modules, see “Interface Modules” on page 14.)

The cabling instructions given below reproduce the configuration shown in Figure 9. However, this is not the only possible configuration. In addition, the instructions assume that you have configured all physical ports and interfaces through the Console port before cabling the device to a network. (For fiber-optic networks, use optical cables for all network connections.)

The ports and interfaces are configured through the Console port as follows:

```
set interface ether1/1 zone dmz
set interface ethernet2/1 zone untrust
set interface ethernet3/8 zone trust
set interface mgt manage
save
```

To add an ISG 2000 to your network:

1. Connect an RJ-45 crossover cable from the Trust interface (**ethernet3/8**) to the internal switch, router, or hub.

NOTE: Check your switch, router, hub, or computer documentation before you attempt to add any new device to a LAN, check the documentation to find out if you should first switch off the power to the device.

---

2. Connect an optical cable from the Untrust interface (**ethernet1/1**) to the external router. You can also connect to the untrusted network remotely using the Console port with an RJ-45 straight-through serial cable or an external modem.

3. Connect an optical cable from the DMZ interface (**ethernet2/2**) to the DMZ switch, router, or hub.

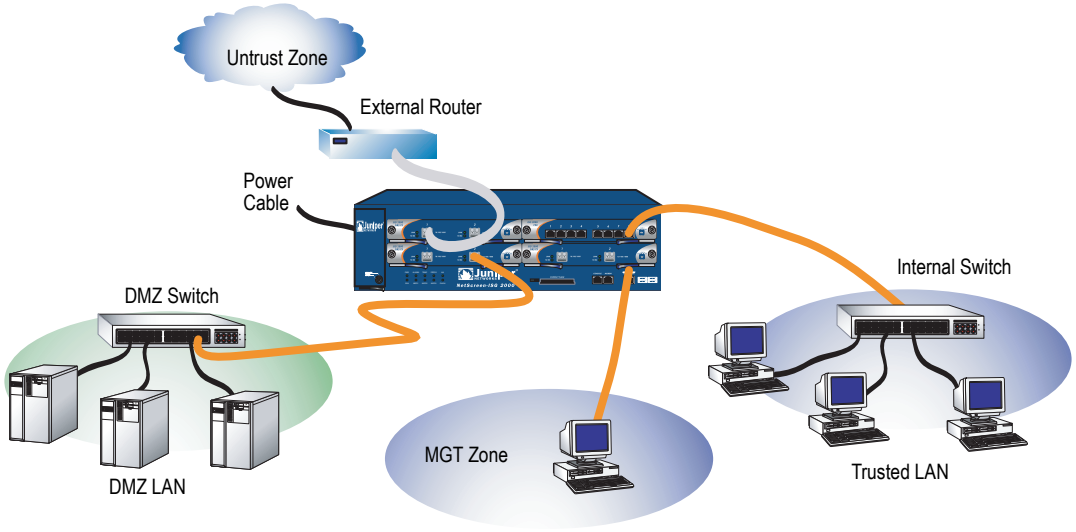
4. Connect an RJ-45 straight-through cable from the MGT port to a workstation in the MGT zone (the default IP address is 192.168.1.1/24).

5. Press the power switch to the ON position.

6. After the ISG 2000 starts up, the POWER, STATUS, and LINK LEDs should light up as follows:

   - The POWER LED for each deployed PSU glows green.
   - The STATUS LED blinks green.
   - The top LINK LED for each interface blinks green. (For more details about interpreting the Link Status LEDs, see “Interface Modules” on page 14.)

Figure 9: Basic Network Connection



Connecting the Modem Port

You can connect to the Untrusted network with an RJ-45 straight-through serial cable and an external modem.

Chapter 3

Configuring a Device

This chapter describes how to configure an ISG 2000 device in your network. It includes the following sections:

NOTE: After you configure a device and verify connectivity through the remote network, you must register your product at http://www.juniper.net/customers/support/ so certain ScreenOS services, such as Deep Inspection Signature Service and Antivirus (purchased separately), can be activated on the device. After registering your product, use the WebUI to obtain the subscription for the service. For more information about registering your product and obtaining subscriptions for specific services, refer to the *Concepts & Examples ScreenOS Reference Guide* for the ScreenOS version running on the device.

Default Device Settings

The ISG 2000 device supports a maximum of 24 ports, each of which can serve as a physical interface. You can configure the Ethernet ports to serve as virtual (*logical*) interfaces. The interfaces that can be configured on the ISG 2000 device are listed in the following tables.

Table 4: Default Interface-to-Zone Bindings

Port Label	Interface	Zone
MGT	mgt (default IP address is 192.168.1.1/24)	MGT
Console	NA	NA
Modem	serial	Untrust
Interface Modules	ethernet*n1/n2* (*n1* is the slot number and *n2* is the physical port number)	Null

Table 5: Logical Interface Naming

Interface Type	Description
Ethernet interfaces	**ethernetn1**/*n2* specifies a physical Ethernet interface.
	ethernetn1/*n2.n3* specifies a sub-interface.
Layer-2 interfaces	**vlan1** specifies the interface used for VPNs while the device is in Transparent mode.
Tunnel interfaces	**tunnel.***n* specifies a tunnel interface. Use this interface for VPN traffic.
Functional interface	**mgt** specifies an interface bound to the MGT zone. The default IP address of this interface is 192.168.1.1/24.

NOTE: We strongly recommend that you change the default IP address and subnet mask for the mgt interface.

The default IP address and subnet mask settings for ISG 2000 interfaces are 0.0.0.0 and 0.0.0.0, respectively. The exception is the mgt interface, a special interface used only for device management. The default IP address and subnet mask settings for the mgt interface are 192.168.1.1 and 255.255.255.0, respectively.

For all operational modes, it is advisable to change the IP address and subnet mask for the mgt interface and to use this interface exclusively for out-of-band management.

To access the vlan1 interface in Transparent mode, you must change the IP address and subnet mask of vlan1 interface to match your current network. In Transparent mode, *only* the mgt and vlan1 interfaces can have a new IP address and subnet mask. All other interfaces must keep their default IP address and subnet mask settings (0.0.0.0 and 0.0.0.0, respectively). To access the vlan1 interface, you must change the IP address and subnet mask of vlan1 interface to match the IP address of your current network.

In Route mode (with or without NAT), at least two Ethernet interfaces must have new IP addresses and subnet masks.

For information on configuring the operational modes, refer to the *Concepts & Examples ScreenOS Reference Guide*.

Accessing a Device

You can configure and manage a device in several ways:

- Console: The Console port on the device allows you to access the device through a serial cable connected to your workstation or terminal. To configure the device, you enter ScreenOS command line interface (CLI) commands on your terminal or in a terminal-emulation program on your workstation.
- WebUI: The ScreenOS Web user interface (WebUI) is a graphical interface available through a browser. To initially use the WebUI, the workstation on which you run the browser must be on the same subnetwork as the device. You can also access the WebUI through a secure server using Secure Sockets Layer (SSL) with secure HTTP (HTTPS).
- Telnet/SSH: Telnet and SSH are applications that allow you to access devices through an IP network. To configure the device, you enter ScreenOS CLI commands in a Telnet session from your workstation. For more information, refer to the *Concepts & Examples ScreenOS Reference Guide*.
- Network and Security Manager (NSM): NSM is a Juniper Networks enterprise-level management application that enables you to control and manage Juniper Networks firewall/IPSec VPN devices. For instructions on how to manage your device with NSM, refer to the Network and Security Manager documentation at http://www.juniper.net/techpubs/software/management/security-manager.

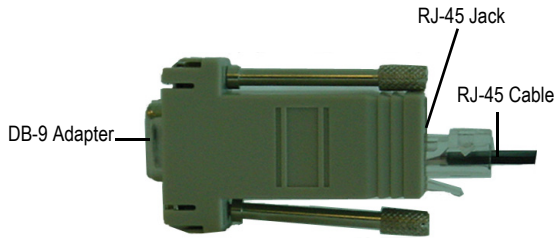
Using a Console Connection

NOTE: Use a straight-through RJ-45 CAT5 serial cable with a male RJ-45 connector to plug into the Console port on the device.

To establish a console connection:

1. Plug the female end of the supplied DB-9 adapter into the serial port of your workstation. (Be sure that the DB-9 is inserted properly and secured.) Figure 10 shows the type of DB-9 connector that is required.

Figure 10: DB-9 Adapter



2. Plug the male end of the RJ-45 CAT5 serial cable into the Console port on the ISG 2000. (Be sure that the other end of the CAT5 cable is inserted properly and secured in the DB-9 adapter.)

3. Launch a serial terminal-emulation program on your workstation. The required settings to launch a console session are as follows:

   - Baud rate: 9600
   - Parity: None
   - Data bits: 8
   - Stop bit: 1
   - Flow Control: None

4. If you have not yet changed the default login for the login name and password, enter **netscreen** at both the login and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive)

   For information on how to configure the device with the CLI commands, refer to the *Concepts & Examples ScreenOS Reference Guide*.

5. (Optional) By default, the console times out and terminates automatically after 10 minutes of idle time. To remove the timeout, enter **set console timeout 0**.

6. Once the command prompt is displayed, the device is ready to be configured, See “Basic Device Configuration” on page 32 to complete the initial device configuration.

Using Telnet

To establish a Telnet connection:

1. Connect your workstation to the MGT port (mgt interface) on the device.

2. Ensure that your workstation is configured for DHCP or is statically configured with an IP address in the 192.168.1.0/24 subnet.

3. Start a Telnet client application to the IP address for the mgt interface (the default IP address is 192.168.1.1). For example, enter **telnet 192.168.1.1**.

   The Telnet application displays the login prompt.

4. If you have not yet changed the default login for the login name and password, enter **netscreen** at both the login and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive)

5. (Optional) By default, the console times out and terminates automatically after 10 minutes of idle time. To remove the timeout, enter **set console timeout 0**.

6. Once the command prompt is displayed, the device is ready to be configured, See "Basic Device Configuration" on page 32 to complete the initial device configuration.

Using Dialup

Each ISG 2000 device provides a modem port that allows you to establish a remote CLI session using a dialup connection through a 9600 bps modem. Dialing into the modem establishes a dialup CLI connection. You must use an RJ-45–to–DB-9 (female-to-male) serial cable with a null modem adapter.

NOTE: The terminal type for dialup sessions must be vt100. For example, in Hilgraeve HyperTerminal, select **Connect > Remote device > vt100** from the Term Type menu.

Using the WebUI

To use the WebUI, the workstation from which you are managing the device must initially be on the same subnetwork as the device. To access the device with the WebUI:

1. Connect your workstation to the MGT port (mgt interface) on the device.
2. Ensure that your workstation is configured for Dynamic Host Configuration Protocol (DHCP) or is statically configured with an IP address in the 192.168.1.0/24 subnet.
3. Launch your browser, enter the IP address for the mgt interface (the default IP address is 192.168.1.1/24), then press **Enter**.

   The WebUI application displays the login prompt.
4. If you have not yet changed the default login for the admin name and password, enter **netscreen** at both the admin name and password prompts. (Use lowercase letters only. The admin name and password fields are both case-sensitive.)

Basic Device Configuration

This section describes the following basic configuration settings:

- Root Admin Name and Password
- Date and Time
- Administrative Access
- Hostname and Domain Name
- Default Route
- Management Interface IP Address
- Management Services
- Trust Zone Interface IP Address

- Untrust Zone Interface IP Address
- Policy Configuration
- Device Alarm
- File Transfers

Root Admin Name and Password

The root admin user has complete privileges for configuring an ISG 2000 device. We recommend that you change the default root admin name and password (both **netscreen**) immediately.

To change the root admin name and password, use the WebUI or CLI as follows:

WebUI

Configuration > Admin > Administrators > Edit (for the Administrator Name **netscreen**): Enter the following, then click **OK**:

Administrator Name:
Old Password: **netscreen**
New Password:
Confirm New Password:

NOTE: Passwords are not displayed in the WebUI.

CLI

```
set admin name name
set admin password pswd_str
save
```

Date and Time

The time settings on an ISG 2000 device affect events such as the setup of VPN tunnels. The easiest way to set the date and time on the device is to use the WebUI to synchronize the device system clock with the workstation clock.

To configure the date and time on a device, use the WebUI or CLI as follows:

WebUI

1. Configuration > Date/Time: Click the Sync Clock with Client button.

   A pop-up message prompts you to specify if you have enabled the daylight saving time option on your workstation clock.

2. Click **Yes** to synchronize the system clock and adjust it according to daylight saving time, or click **No** to synchronize the system clock without adjusting for daylight saving time.

CLI

```
set clock
save
```

The **set clock** CLI command allows you to manually enter the date and time for the device.

Administrative Access

By default, anyone in your network can manage a device if they know the admin name and password.

To configure the device to be managed only from a specific host on your network, use the WebUI or CLI as follows:

WebUI

Configuration > Admin > Permitted IPs: Enter the following, then click **Add**:

IP Address/Netmask: *ip_addr/mask*

CLI

```
set admin manager-ip ip_addr/mask
save
```

Hostname and Domain Name

The domain name defines the network or subnetwork to which a device belongs, while the hostname refers to a specific device. The hostname and domain name together uniquely identify the device in the network.

To configure the hostname and domain name on a device, use the WebUI or CLI as follows:

WebUI

Network > DNS > Host: Enter the following, then click **Apply**:

Host Name: *hostname*
Domain Name: *domain-name*

CLI

```
set hostname hostname
set domain domain-name
save
```

Default Route

The default route is a static route used to direct packets addressed to networks that are not explicitly listed in the routing table. If a packet arrives at the device with an address for which the device does not have routing information, the device sends the packet to the destination specified by the default route.

To configure the default route on the device, use the WebUI or CLI as follows:

WebUI

Network > Routing > Destination > New (trust-vr): Enter the following, then click **OK**:

IP Address/Netmask: 0.0.0.0/0.0.0.0
Next Hop
    Gateway: (select)
    Interface: ethernet1/1 (select)
    Gateway IP Address: *ip_addr*

CLI

```
set route 0.0.0.0/0 interface ethernet1/1 gateway ip_addr
save
```

Management Interface IP Address

The default IP address and subnet mask settings for the mgt interface are 192.168.1.1 and 255.255.255.0, respectively. If you do not want to use this default IP address, you need to assign a new interface address that matches your current network. We recommend using the MGT interface exclusively for management.

To set the IP address of the MGT port to 10.100.2.183/16, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > Edit (for mgt): Enter **10.100.2.183/16** in the IP address and netmask fields, then click **Apply**.

CLI

```
set interface mgt ip 10.100.2.183/16
save
```

Management Services

ScreenOS provides services for configuring and managing a device, such as SNMP, SSL, and SSH, which you can enable for each interface.

To configure the management services on the device, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > Edit (for mgt): Under **Management Services**, select or clear the management services you want to use on the interface, then click **Apply**.

CLI

```
set interface mgt manage web
unset interface mgt manage snmp
save
```

Trust Zone Interface IP Address

The ISG 2000 device can communicate with your protected network through an interface bound to the Trust zone. To allow an interface to communicate with internal devices, you must assign it the IP address and subnet mask for your protected network.

To set the ethernet3/1 interface to communicate with your trusted network, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > Edit (for ethernet3/1): Enter the following, then click **Apply**:

Zone Name: Trust (select)
IP Address/Netmask: 10.250.2.1/16

CLI

```
set interface ethernet3/1 zone trust
set interface ethernet3/1 ip 10.250.2.1/16
save
```

Untrust Zone Interface IP Address

The ISG 2000 device can communicate with external (untrusted) devices through an interface usually bound to the Untrust zone. To allow an interface to communicate with external devices, you must assign it a public IP address.

To set the ethernet1/1 interface to communicate with external devices, use the WebUI or CLI as follows:

WebUI

Network > Interfaces > Edit (for ethernet1/1): Enter the following, then click **Apply**:

Zone Name: Untrust (select)
IP Address/Netmask: 172.16.20.1/16

CLI

```
set interface ethernet1/1 zone untrust
set interface ethernet1/1 ip 172.16.20.1/16
get interface ethernet1/1
save
```

Policy Configuration

By default, the ISG 2000 device does not allow inbound or outbound traffic or traffic to or from the DMZ. To permit (or deny) traffic, you must create access policies.

CAUTION: Your network might require a more restrictive policy than the example provided in this guide. This example is not a requirement for initial configuration. For detailed information about access policies, refer to the *Concepts & Examples ScreenOS Reference Guide.*

To create and save an access policy that permits all kinds of outbound traffic from any host in your trusted LAN to any device on the untrusted network, use the WebUI or CLI as follows:

WebUI

Policies > (From: Trust To: Untrust) > New: Enter the following, then click **OK**:

Name: Trust-Untrust
Source Address: Any (select)
Destination Address: Any (select)
Service: Any (select)
Action: Permit (select)

CLI

```
set policy from trust to untrust any any any permit
save
```

Device Alarm

The ISG 2000 device allows you to configure the device alarm, an audible warning that sounds when a device fails or a hazardous event occurs.

To specify which failures and events trigger the device alarm, use the **set chassis audible-alarm** *string* CLI command**.** Table 6 describes the keywords available for the **set chassis** CLI command.

Table 6: Set Chassis Keywords

Keyword	Meaning
all	Enables all device alarms
battery	Sets the device alarm to sound when a battery fails
fan-failed	Sets the device alarm to sound when a fan fails
power-failed	Sets the device alarm to sound when a power supply fails
temperature	Sets the device alarm to sound when the temperature goes outside the acceptable range

File Transfers

To download files from or upload files to the device, use the WebUI or CLI as follows:

WebUI

Configure > Update > ScreenOS/Keys or Config File > Select the type of file you wish to transfer, browse for the file that you wish to upload onto the device, then click **Apply**.

Once you click **Apply**, the device restarts. This process could take up to several minutes.

CLI

save { software | config } from { flash | slot1 *filename* } to { flash | slot1 *filename* }

where **flash** refers to internal flash memory, **slot1** refers to the compact flash slot, and *filename* is the name of the software or configuration file on the card.

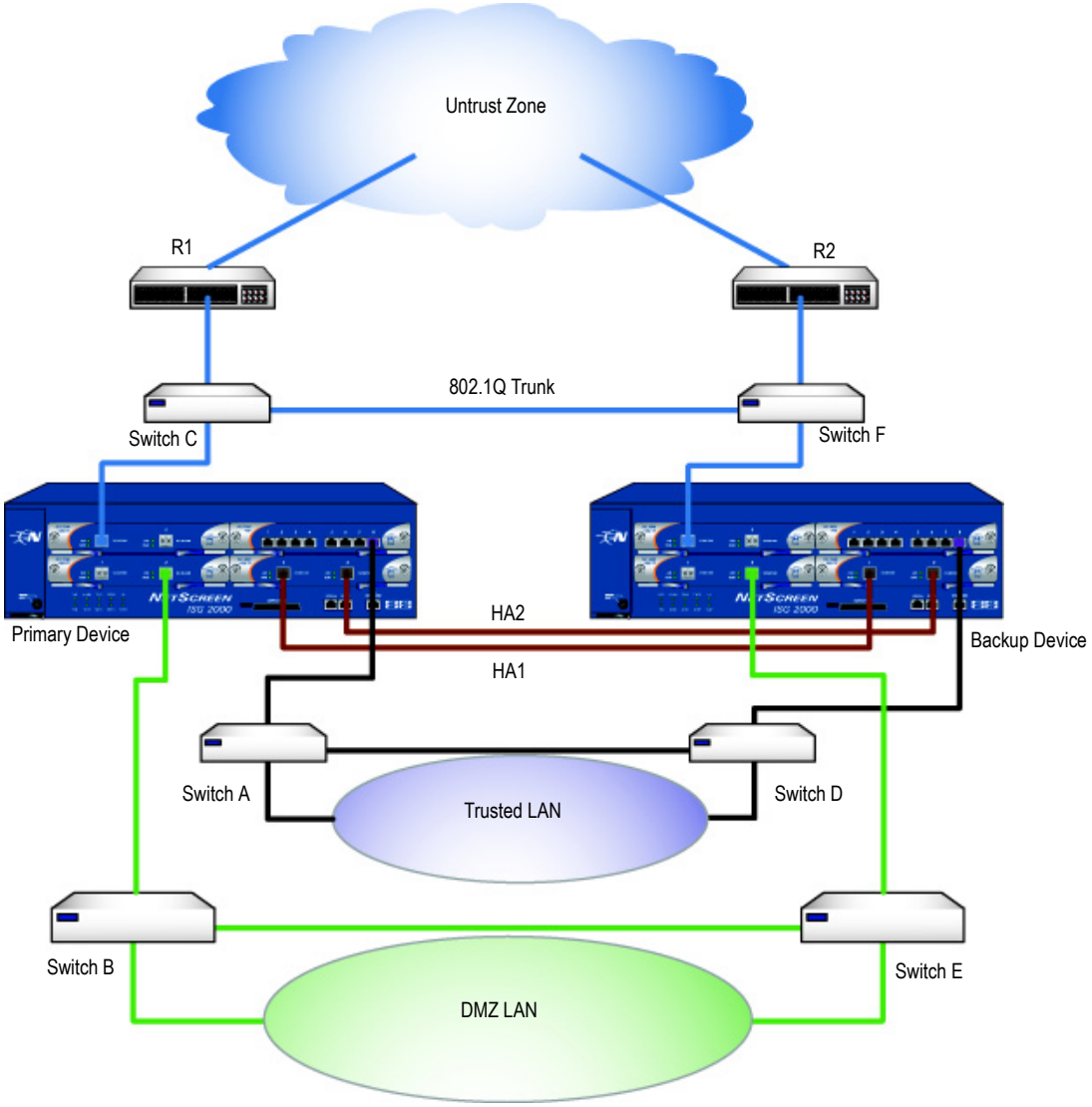
High Availability Configuration

There are no dedicated high availability (HA) interfaces on the ISG 2000 device; therefore, you must select and configure the HA ports once the device is running. HA ports allow you to cable two devices together and configure them to work as a *redundant group*. A redundant group consists of one primary device and one backup device. If the primary device fails, the backup device takes over as the new primary, thus avoiding interruption of services. Any number and type of interfaces, from the four interface modules, can be used as HA ports. The backup device must have the same interface modules installed and ScreenOS configuration as the primary device for HA to work correctly.

NOTE: We recommend that you use mini-GBIC interface modules when possible. Do not mix mini-GBIC and 10/100 Mbps ports. If you do not have a mini-GBIC interface module, you should use at least two 10/100 Mbps interfaces. For more information about HA configuration, refer to the *Concepts & Examples ScreenOS Reference Guide.*

The ISG 2000 supports a maximum port count of 28. If there are eight-port 10/100 modules in each I/O slot, then ports 5 through 8, in slot 4, are disabled. Under this circumstance, these ports are unavailable for firewall and HA functions.

Figure 11: HA Cabling Connections



NOTE: The provided cabling instructions reproduce the configuration shown in Figure 11; however, this is not the only possible HA configuration. In addition, the instructions assume that all physical ports and interfaces are still at their defaults. If you have changed the port and interface settings, the instructions might not work properly.

To cable two ISG 2000 security devices together for HA and connect them to the network:

1. Connect a 10/100Base-T crossover cable from the preferred HA1 port on the primary device to the preferred HA1 port on the backup device.

2. Connect a 10/100Base-T crossover cable from the preferred HA2 port on the primary device to the preferred HA2 port on the backup device.

Configuring HA Ports

3. Set the HA interface by executing the following command on each device, for example:

```
set interface ethernet4/1 zone ha
set interface ethernet4/2 zone ha
```

Master Unit

4. Connect a crossover cable from **ethernet3/8** to **Switch A**.

5. Connect an optical cable from **ethernet2/2** to **Switch B**.

6. Connect an optical cable from **ethernet1/1** to **Switch C**.

Backup Unit

7. Connect a crossover cable from **ethernet3/8** to **Switch D**.

8. Connect an optical cable from **ethernet2/2** to **Switch E**.

9. Connect an optical cable from **ethernet1/1** to **Switch F**.

Switches

10. Cable together **Switch A** and **Switch D**.

11. Cable together **Switch B** and **Switch E**.

12. Cable together **Switch C** and **Switch F**.

13. Cable **Switch C** to **R1**.

14. Cable **Switch F** to **R2**.

NOTE: The switch ports must be defined as 802.1Q trunk ports, and the external routers must be able to use either Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP). For the best configuration method, refer to the documentation for your switch or router.

---

15. Press the power switch to the ON position for both devices.

Restarting the Device

You may need to restart the device in order to implement new features, such as when you change between route and transparent mode or when you add new license keys.

The following sections describe two methods of restarting the device:

- "Restarting the Device with the CLI Reset Command" on page 42
- "Restarting the Device with the WebUI" on page 42

Restarting the Device with the CLI Reset Command

To restart the device with the CLI reset command:

1. Establish a console session with the device as described in "Using a Console Connection" on page 28 or "Using Telnet" on page 30.

   At a Windows workstation, the easiset way of opening a console connection is to choose **Start > Run** and enter **telnet** *ip_address*.

   The device prompts you for your login and password.

2. If you have not yet changed the default username and password, enter **netscreen** at both the login and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive.)

3. At the console prompt, enter:

   reset

   The device prompts you to confirm the reset:

   System reset, are you sure? y/[n]

4. Enter **Y**.

   The device restarts.

Restarting the Device with the WebUI

To restart the device with the WebUI:

1. Launch your browser and enter the IP address for the management interface (the default IP address is **192.168.1.1**), then press **Enter**.

   The WebUI application displays the login prompt.

2. If you have not yet changed the default username and password, enter **netscreen** at both the login and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive.)

3. In the WebUI, choose:

   Configuration > Update > ScreenOS/Keys

4. Click **Reset**.

   An alert box prompts you to confirm that you want to reset the device.

5. Click **OK**.

   The device resets. Also, an alert box prompts you to leave your browser open for a few minutes and then log back into the device.

Resetting a Device to Factory Defaults

If you lose the admin password, or you need to clear the configuration of your device, you can reset the device to its factory default settings. Resetting the device destroys any existing configurations and restores access to the device.

CAUTION: Resetting the device deletes all existing configuration settings and disables all existing firewall and VPN services.

NOTE: By default, the device recovery feature is enabled. You can disable it by entering the CLI **unset admin device-reset** command. Also, if the security device is in FIPS mode, the recovery feature is automatically disabled.

You can restore the device to its default settings using one of these methods:

- Using the device serial number
- Using the CLI **unset all** command

The following sections describe how to use these methods to reset the device to its factory defaults.

Device Serial Number

To use the device serial number to reset the device to its factory defaults:

1. Start a Console session as described in "Using a Console Connection" on page 29.
2. At the Login prompt, enter the device serial number.
3. At the Password prompt, enter the serial number again. The following message appears:

   !!! Lost Password Reset !!! You have initiated a command to reset the device to factory defaults, clearing all current configuration and settings. Would you like to continue? y/[n]

4. Press the **y** key. The following message appears:

   !! Reconfirm Lost Password Reset !! If you continue, the entire configuration of the device will be erased. In addition, a permanent counter will be incremented to signify that this device has been reset. This is your last chance to cancel this command. If you proceed, the device will return to factory default configuration, which is: device IP: 192.168.1.1; username: netscreen, password: netscreen. Would you like to continue? y/[n]

5. Press the **y** key to reset the device.

The system now resets and returns to the login prompt; the default login name and password are both reset to **netscreen**.

unset all

To use the CLI **unset all** command, you will need to know the login name and password. To reset the device to its factory defaults:

1. Start a Console session as described in “Using a Console Connection” on page 29, then log in.

2. At the command prompt, enter **unset all**. The following message is displayed:

   ```
   Erase all system config, are you sure y/[n] ?
   ```

3. Press **y**

4. Enter **reset**. Press **n** for the first question and **y** for the second question:

   ```
   Configuration modified, save? [y]/n
   System reset, are you sure? y/[n]
   ```

The system now resets and returns to the login prompt; the default login name and password are both reset to **netscreen**.

Chapter 4

Intrusion Detection and Prevention

Intrusion Detection and Prevention (IDP) is a mechanism for filtering the traffic permitted by firewall policies. IDP uses a variety of techniques such as examining Layer 3 and 4 packet headers and Layer 7 application content and protocol characteristics in an effort to detect and prevent any attacks or anomalous behavior that might be present in permitted traffic. For more information about IDP, refer to the *ISG 2000 Getting Started with IDP Guide*.

This section explains the minimum configuration needed to connect to Network and Security Manager (NSM). You can use NSM, the Web user interface (WebUI), or the command line interface (CLI) to install an IDP license key; however, to configure IDP for an ISG 2000 device, you must use NSM.

NOTE: You must register your product at www.juniper.net/customers/support/ so that you can activate specific services such as IDP. After registering your product, purchase a license key from your value added reseller (VAR), and then use NSM, the WebUI, or the CLI to load the key. For information about registering your product and obtaining and loading license keys, refer to the *Concepts & Examples ScreenOS Reference Guide*.

When you install an IDP license key, the ISG 2000 automatically disables Deep Inspection (DI).

Minimum Configuration for a Network and Security Manager Connection

Before you can manage an ISG 2000 device with NSM, you need to set up the ISG 2000 on the network so that NSM can connect to it. To set the minimum configuration options needed to use NSM:

1. Set an IP address for the interface through which NSM can connect to the ISG 2000:

   ```
   set interface ethernet1/1 zone untrust
   set interface ethernet1/1 ip 1.1.1.1/30
   ```

2. If there is a network-forwarding device between the ISG 2000 and the NSM server, set a route through that device to the server with the following CLI command:

   ```
   set vrouter trust-vr route 0.0.0.0/0 interface ethernet1/1 gateway 1.1.1.2
   ```

3. Enable the ISG 2000 for management from NSM. This is enabled by default.

   ```
   set nsm enable
   save
   ```

You can now connect to the ISG 2000 device through ethernet1/1 from NSM and continue configuring the device.

For instructions on how to manage a device with NSM, refer to the Network and Security Manager documentation at http://www.juniper.net/techpubs/software/management/security-manager.

Chapter 5

Servicing a Device

This chapter describes service and maintenance procedures for your ISG 2000 device. It includes the following sections:

NOTE: For safety warnings and instructions, refer to the *Juniper Networks Safety Guide*. The guide warns you about situations that could cause bodily injury. When working on any equipment, be aware of the hazards involved with electrical circuitry, and follow standard practices for preventing accidents.

Required Tools and Parts

To replace a component on an ISG 2000 device, you need the following tools and parts:

- Electrostatic bag or antistatic mat
- Electrostatic discharge (ESD) grounding wrist strap
- Number-2 phillips screwdriver, 1/8-inch

Interface Modules

This section provides instructions on how to service the interface modules on an ISG 2000 device.

To remove an interface module from a slot:

WARNING: When inserting or removing interface modules, be sure that the power is in the OFF position.

1. Unscrew the thumbscrews on each side of the interface module.
2. With your thumbs, pull out the blue locking levers (see Figure 12).

Figure 12: Interface Locking Levers

3. Grip the levers, then gently slide the module straight out (see Figure 13).

4. If you are not reinstalling an interface module into the empty slot, install a blank faceplate over the slot to maintain proper airflow.

Figure 13: Interface Removal

WARNING: When inserting and removing a module in slot 2, take care that the electromagnetic interference (EMI) fingers located along the top edge of the front wall of the interface module do not catch on the lower edge of the module above the module in slot 1.

To insert an interface module into a module slot:

WARNING: When inserting or removing interface modules, be sure that the power is in the OFF position.

1. Align the side edges of the module with the grooves in the side walls of the slot (see Figure 14).

Figure 14: Interface Slot Alignment

2. Slide the module in until it is forced to stop.

WARNING: When inserting and removing a module in slot 2, take care that the electromagnetic interference (EMI) fingers located along the top edge of the front wall of the interface module do not catch on the lower edge of the module above the module in slot 1.

3. With your thumbs, push in the locking levers to secure the module.

Figure 15: Interface Locked

CAUTION: If you push the latch before it contacts the ridge on the bay wall, the locking tab clicks into place prematurely, and you will not be able to properly seat the interface module.

4. Tighten the thumbscrews on each side of the interface module.

Power Supply Units

An ISG 2000 device supports two redundant, fault-tolerant, auto-switching power supply units (PSUs). The PSUs are hot-swappable, so you can remove or replace one without interrupting device operation.

You can order an ISG 2000 with one or two PSUs: DC or AC. Although the ISG 2000 can run with one PSU, it is advisable to install two. This practice minimizes the chance of device failure due to an individual PSU failure.

WARNING: Do not mix the PSU types because doing so could seriously damage the device.

AC Power Supply Unit Replacement

To install and connect the AC PSU:

1. Press the power switch to the OFF position.
2. Unplug the cord from the PSU.
3. Loosen the thumbscrews on the sides of the PSU by turning them counterclockwise.
4. Lift the handle and pull the PSU straight out.
5. Slide the new PSU into the power-supply compartment at the back of the ISG 2000.
6. Fasten the PSU to the device by tightening the thumbscrews.
7. Connect the female end of a standard power cord to the male connector on the back of the PSU.

8. Connect the power cord to a standard 100-240-volt power outlet.

NOTE: Whenever you deploy two PSUs to an ISG 2000, connect each to a different power source. Each PSU is intended to receive power from separate feeds.

9. Press the power switch to the ON position.

DC Power Supply Unit Replacement

NOTE: If both PSUs are installed and either of them is off, the ALARM LED on the front panel glows red. This warning indicates that maximum device reliability requires all installed PSUs to be operational.

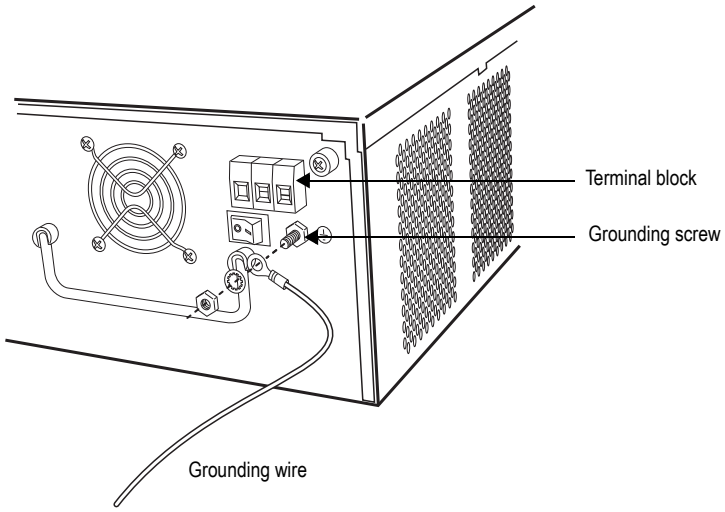
WARNING: You must shut off current to the DC feed wires before connecting the wires to the PSUs. Also, make sure that the ON/OFF switch is in the OFF position.

To connect a DC PSU to a grounding point at your site:

1. Loosen or remove the hex nut from the grounding screw by rotating the hex nut counterclockwise.

2. Place the ground lug on the grounding screw, and tighten the hex nut by rotating it clockwise until it holds firmly.

Figure 16: Adding the Ground Lug

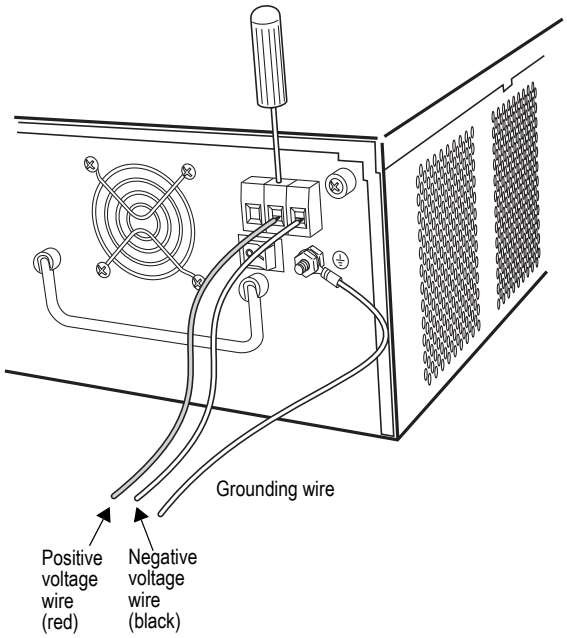


3. Connect the other end of the grounding wire to a grounding point at your site.

To connect DC power-feed wires to the terminal block:

1. To open the three connectors on the terminal block so that they can receive wire feeds, use the number-2 phillips screwdriver to turn the retaining screws counterclockwise.

Figure 17: Opening the Connectors



2. Insert a 0V DC (positive voltage) return wire into the center COM connector and a -48V DC power-feed wire into either the left or the right connector.

3. Fasten the screws over the connectors.

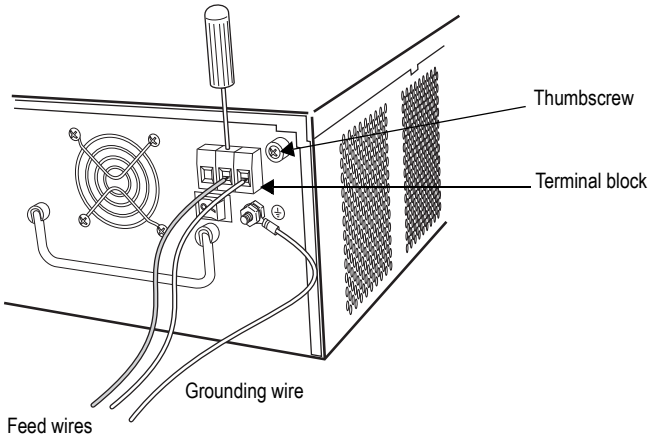
4. Press the power switch to the ON position.

NOTE: If both PSUs are installed and either of them is off, the ALARM LED on the front panel glows red. This warning indicates that maximum device reliability requires all installed PSUs to be operational.

To replace one DC PSU:

1. Loosen the retaining screws on the terminal block and remove the feed wires.
2. Loosen the hex nut on the grounding screw and remove the grounding wire.

Figure 18: Removing the Feed Wires and Grounding Wire



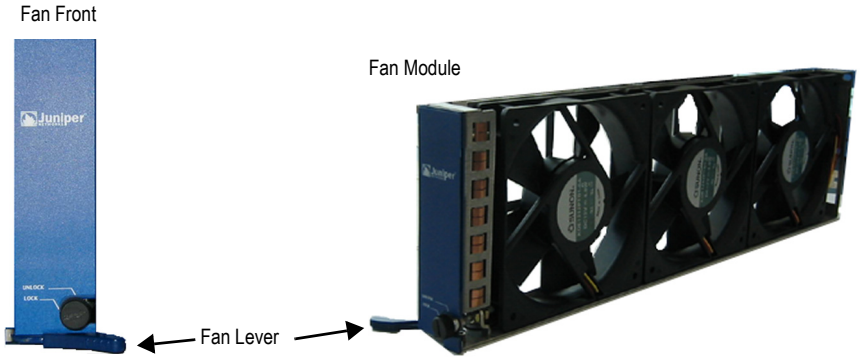
3. Loosen the thumbscrews by turning them counterclockwise to release the PSU.
4. Lift the handle and, gripping the handle, pull the PSU straight out.
5. Slide the new power supply into one of the power compartments in the back of the device.
6. Fasten the PSU to the device by tightening the thumbscrews clockwise.
7. If you want to install two PSUs, repeat steps 1 and 2.

Fan Tray

NOTE: During the one-year warranty period, you can obtain a replacement fan module by contacting Juniper Networks Technical Support. After the warranty period, contact the Juniper Networks Sales department.

You only need to replace the fan module when a failure occurs. When this happens, the FAN LED glows red, and the device generates an event alarm and an SNMP trap.

Figure 19: Fan Module



To remove the fan module:

1. Pull the fan lever until it is fully extended.
2. Grip the sides, then gently slide the assembly straight out (see Figure 20).

WARNING: Do not remove the fan module while the fans are still spinning.

Figure 20: Removing the Fan

3. Insert the new fan module in the fan bay, then push it straight in.
4. Secure the fan module in place by pushing the fan lever flat against the front panel.

Fan-Tray Filter

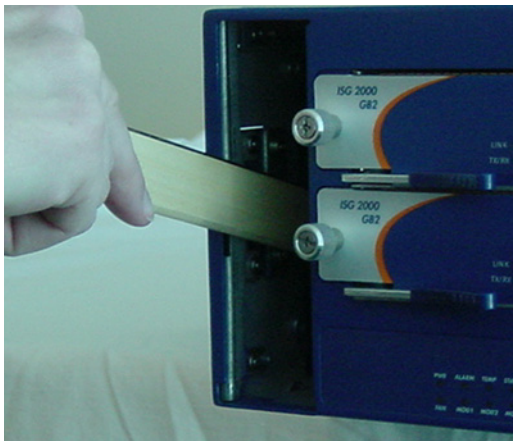
Before you replace the fan-tray filter, make sure you have the following tools:

- Flashlight or other light source
- 18-inch wooden ruler

To replace the fan-tray filter:

1. Remove the fan tray (see “Fan Tray” on page 56).
2. Pull the front edge of the filter from the Velcro backing, located on the device wall.
3. Insert a wooden ruler between the filter and the device wall to loosen the filter (see Figure 21).

Figure 21: Loosening the Fan-Tray Filter



4. Push the wooden ruler toward the back of the device, gently lifting the filter as you proceed.
5. Once the filter is separated from the Velcro backing, use your fingers to pull the filter out of the fan-tray slot (see Figure 22).

Figure 22: Removing the Fan-Tray Filter

6. Carefully insert a new filter into the device. Use the wooden ruler as an aid to guide the back edge of the filter to reach the end of the device wall.

7. Once the filter is fully inserted, push the wooden ruler against the surface of the filter several times to ensure that the filter is secure against the Velcro backing on the device wall.

CAUTION: Make sure that the filter is secure against the device wall; otherwise, the filter will tear when you reinstall the fan.

8. Insert the new fan module in the fan bay, then push it straight in.

9. Secure the fan module in place by pushing the fan lever flat against the front panel.

NOTE: If the top cover of the device is accessible, you may find it easier to remove the cover and access the filter from the top of the device.

NOTE: An ISG 1000 or ISG 2000 device can operate without a fan-tray filter; however, without the filter the device does not comply with NEBS standards.

Cables and Transceivers

This section provides instructions on how to service the cables and transceivers on the interface modules.

Gigabit Ethernet Cables

To connect a Gigabit Ethernet cable to a mini-GBIC transceiver port:

1. If you have not already done so, remove the two plastic fiber-protection caps from the ends of the cable.

2. Hold the cable connector between your thumb and forefinger, with your thumb on top and your forefinger underneath. (Do not press the release on top of the connector.)

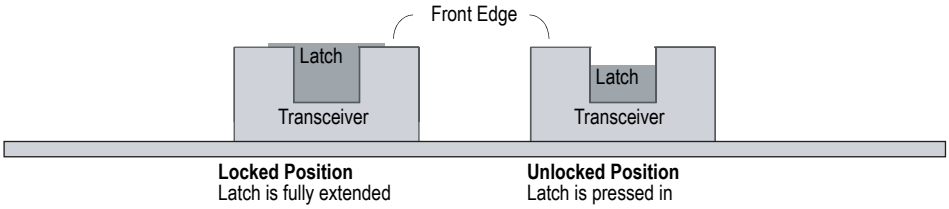
3. Slide the connector into the transceiver port until it clicks into place. Because the fit is close, you might have to apply some force to insert the connector. To avoid damaging the connector, apply force evenly and gently (see Figure 23).

Figure 23: Sliding the Connector into the Transceiver Port

To remove the cable from the transceiver port:

1. Make sure the transceiver latch is in a secured, locked position (the latch is flat against the front of the transceiver). Otherwise, when you attempt to remove the cable, the transceiver might come out with the cable still attached.

Figure 24: Transceiver Latch



2. Hold the connector between your thumb and forefinger, with your thumb on top and your forefinger underneath.

3. Using your thumb, press the connector release down, then forward. This action loosens the connector from the transceiver port (see Figure 25).

Figure 25: Ejecting the Cable

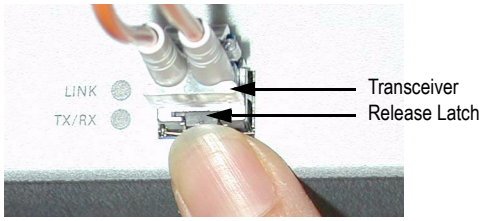
4. Gently but firmly pull the clip from the transceiver port.

Mini-GBIC Transceiver

To remove a mini-GBIC transceiver from an interface module:

1. Push in the transceiver release latch (located on the underside of the transceiver) until it locks into place, disengaging the transceiver (see Figure 26).

Figure 26: Releasing the Transceiver



2. Grasp the transceiver at both sides, and pull the transceiver toward you to remove it from the interface module.

To install a mini-GBIC transceiver into an interface module, holding the transceiver with the label face up, then insert it into the transceiver slot (see Figure 27).

Figure 27: Installing the Transceiver

Security Modules

Security modules are high-performance-processing subdevices that increase the performance of the ISG 2000 for high CPU-usage services, such as Intrusion Detection and Prevention (IDP).

CAUTION: Before you install or remove a security module, make sure the power is OFF, the power cords are removed, and the device is placed on a stable table.

NOTE: For better signal integrity, use slots 3 through 1, placing the first security module in slot 3. Security Module slots are number Slot 3, Slot 2 and Slot 1 starting from the back of the device.

To install or remove a security module:

1. Remove the top cover from the device. (Remove the three screws located on the sides and the back of the top cover.)

2. Insert the security module into an empty slot, starting with the slot closest to the back of the device, which would be slot 3.

3. After inserting the security module into the slot, use the insertion/extraction handles to correctly install the module into the slot.

Once all of the security modules are installed, replace the cover, install the device in the rack, connect the power cords, and then turn on the power.

Appendix A
Specifications

This appendix provides general system specifications for the ISG 2000. It includes the following sections:

Physical

Table 7 provides the physical specifications for the ISG 2000.

Table 7: Physical Specifications

Height	5.25 in. (13.4 cm)
Depth	23.25 in. (59 cm)
Width	17.5 in. (44.5 cm)
Weight	42 lb (19 kg)

Electrical

Table 8 provides the electrical specifications for the ISG 2000.

Table 8: Electrical Specifications

AC voltage	100 - 240 VAC +/- 10%
DC voltage	-36 to -60 VDC
AC power	250 Watts
DC power	250 Watts
AC input frequency	47 - 63 Hz
Fuse rating	DC PS: 10 Amps/250 Volts; AC PS: 6.3 Amps/250 Volts

WARNING: Certain ports on the device are designed for use as intrabuilding (within-the-building) interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Isssue 4) and require isolation from the exposed outside plant (OSP) cabling. To comply with NEBS requirements and protect against lightning surges and commercial power disturbances, the intrabuilding ports must not be metallically connected to interfaces that connect to the OSP or its wiring. The intrabuilding ports on the device are suitable for connection to intrabuilding or unexposed wiring or cabling only. The addition of primary protectors is not sufficient protection for connecting these interfaces metallically to OSP wiring.

CAUTION: To comply with intrabuilding lightning and surge requirements, intrabuilding wiring must be shielded, and the shield for the wiring must be grounded at both ends.

Environmental

Table 9 provides the environmental specifications for the ISG 2000:

Table 9: Environmental Tolerance

Temperature	Operating
Normal altitude (max is 2,000 ft. (0-3,660 m))	32-113 × F, 0 × - 45 × C
Humidity	10-90% RH, noncondensing

Certifications

Table 10 shows the certifications available for the ISG 2000.

Table 10: ISG 2000 Certifications

Certification Type	Certification Name
NEBS[a]	NEBS Level 3 GR-63-Core: NEBS, Environmental Testing GR-1089-Core: EMC and Electrical Safety for Network Telecommunications Equipment
Safety	CAN/CSA-C22.2 No. 60950-1-03/UL 60950-1, EN 60950-1, IEC 60950-1
EMI	FCC class A, CE class A, C-Tick, VCCI Class A

a.An ISG 1000 or ISG 2000 device can operate without a fan-tray filter; however, without the filter the device does not comply with NEBS standards.

Connectors

Figure 28 shows the location of the pins on the RJ-45 connector.

Figure 28: RJ-45 Pinouts

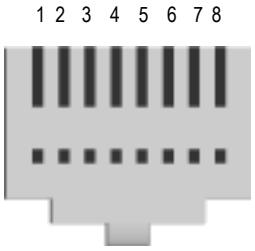


Table 11 lists the RJ-45 connector pinouts.

Table 11: RJ-45 Connector Pinouts

Pin	Name	I/O	Description
1	RTS Out	O	Request To Send
2	DTR Out	O	Data Terminal Ready
3	TxD	O	Transmit Data
4	GND	NA	Chassis Ground
5	GND	NA	Chassis Ground
6	RxD	I	Receive Data
7	DSR	I	Data Set Ready
8	CTS	I	Clear To Send

Figure 29 shows the location of the pins on the DB-9 female connector.

Figure 29: DB-9 Female Connector

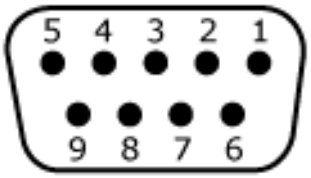


Table 12 provides the DB-9 connector pinouts.

Table 12: DB-9 Connector Pinouts

Pin	Name	I/O	Description
1	DCD	I	Carrier Detect
2	RxD	I	Receive Data
3	TxD	O	Transmit Data
4	DTR	O	Data Terminal Ready
5	GND	NA	Signal Ground
6	DSR	I	Data Set Ready
7	RTS	O	Request To Send
8	CTS	I	Clear To Send
9	RING	I	Ring Indicator

The mini-Gigabit transceivers are compatible with the IEEE 802.3z Gigabit Ethernet standard, and the 10Gbase-R transceivers are compatible with the IEEE 802.3ae standard. Table 13 lists media types and distances for the different types of interfaces used in the ISG 2000.

Table 13: Interface Media Types for Mini-Gigabit Transceivers and 10Gigabit XFP Transceivers

Standard	Media Type	Maximum Distance (in Meters)
1000Base-SX	50/125µ m multimode fiber	500
	50/125µ m multimode fiber	550
	62.5/125µ m multimode fiber	220
	62.5/125µ m multimode fiber	275
1000Base-LX	50/125µ m multimode fiber	550
	62.5/125µ m multimode fiber	550
	9/125µ single-mode fiber	10,000
100Base-TX	Category 5 and higher UTP cable	100
10Gbase-SR	850nm multimode fiber	26-300
10Gbase-LR	1310nm single-mode fiber	10,000

Index

R

S

T

U

W